多変数多項式暗号 2
-安全性解析-

池松 泰彦
(九州大学マス・フォア・インダストリ研究所)

耐量子計算機暗号と量子情報の数理

2022年8月4日

Institute of Mathematics for Industry
Kyushu University

概要

- ✓ 量子計算機の出現により公開鍵暗号が危殆化
- ✓ 多変数多項式暗号(MPKC)がPQCの候補として研究される
- ✓ MQ問題やMinRank問題の難しさを安全性の根拠とする
- ✓ これまで様々なMPKC、特に署名方式が提案されてきた

解説内容 (MPKCの安全性解析)

- MQ問題の求解方法、その計算量評価を解説
- MinRank問題の求解方法、その計算量評価を解説
- 方式特有の構造を利用した攻撃を解説

目次

§1.1 多変数多項式暗号(MPKC)

■ 多変数多項式暗号(Multivariate Public Key Cryptography)

✓ 多変数二次多項式問題(MQ問題)の求解困難性を利用した暗号技術

例: 次の $\mathbb{F}_{31}$ 上の連立二次多項式を考える：

$$p_1 = 11x_1^2 + 24x_1x_2 + 5x_1x_3 + 22x_2^2 + x_2x_3 + 17x_3^2,$$
$$p_2 = 27x_1^2 + 29x_1x_2 + 24x_2^2 + 27x_2x_3 + 19x_3^2,$$
$$p_3 = 4x_1^2 + 6x_1x_2 + x_1x_3 + 25x_2^2 + 27x_2x_3 + 26x_3^2.$$

$$P := (p_1, p_2, p_3) : \mathbb{F}_{31}^3 \longrightarrow \mathbb{F}_{31}^3$$

$(x_1, x_2, x_3) = (0,1,1)$ ➡ $P(0,1,1) = (9,8,16)$ 代入計算は易しい

$P(x_1, x_2, x_3) = (9,8,16)$ ➡ $(x_1, x_2, x_3) = \pm(0,1,1)$ 求解は難しい

✓ 1980年代に日本の松本・今井らにより導入[MI88]

✓ 耐量子計算機暗号の候補として現在活発に研究されている

✓ NIST PQC 標準化計画の中ではUOV系が注目を集めている

NIST would like submissions for signature schemes that have short signatures and fast verification (e.g., UOV).

[MI88] Matsumoto, T et al.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, EUROCRYPT1988

§1.2 MPKCの一般的構成の復習

■ 定義. 二次中心写像

$$f_1(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{i,j}^{(1)} x_i x_j,$$
$$\vdots$$
$$f_m(x_1,\dots,x_n) = \sum_{1\le i\le j\le n} a_{i,j}^{(m)} x_i x_j$$

$F := (f_1,\dots,f_m)\colon \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ を二次写像として，
任意の元 $d \in \mathbb{F}_q^m$ に対して，$F(x) = d$ は少ない計算量で解けるもの.

■ 秘密鍵

$F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ 二次中心写像

$S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$
$T : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ ） ランダムな可逆な線型写像

■ 公開鍵

$P := T \circ F \circ S : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ 二次写像 Fが隠れる
$= (p_1,\dots,p_m)$

署名 メッセージ

$$\begin{tikzcd}
s \in \mathbb{F}_q^n \arrow[r, "P", "\text{検証}"'] & \mathbb{F}_q^m \ni d \arrow[d, "T^{-1}"'] \\
\mathbb{F}_q^n \arrow[u, "S^{-1}"'] & \mathbb{F}_q^m \arrow[l, "\text{署名生成}"', "F^{-1}"]
\end{tikzcd}$$

MQ問題とEIP問題が安全性を支えていると考えられている

§1.3 二次多項式行列表現

■ 二次多項式は右上三角行列で一意に表現可能

$x := (x_1, x_2, x_3)$

例) $f(x) = 11x_1^2 + 24x_1x_2 + 4x_1x_3 + 17x_3^2$

$$= \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \underbrace{\begin{pmatrix} 11 & 24 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 17 \end{pmatrix}}_{U_f \text{と書く}} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

■ しかしこの表現は変数変換と相性が良くない

$$f \circ S(x) = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \cdot \underbrace{S \begin{pmatrix} 11 & 24 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 17 \end{pmatrix} S^t}_{U_{f\circ S} \text{ に一致しない}} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$S(x) = (x_1\ x_2\ x_3) \cdot S$
と行列表示している

■ 二次多項式は対称行列と相性が良い

$$f \longmapsto Q_f \coloneqq U_f + U_f^t$$ f から決まる対称行列

⇒ $$Q_{f \circ S} = S \cdot Q_f \cdot S^t$$

■ 秘密鍵と公開鍵の関係

$F = (f_1, \dots, f_m),\ \ S \colon \mathbb{F}_q^n \to \mathbb{F}_q^n,\ \ T \colon \mathbb{F}_q^m \to \mathbb{F}_q^m$ ：秘密鍵

$P \coloneqq T \circ F \circ S = (p_1, \dots, p_m) \colon \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ ：公開鍵

⇒ $$(p_1, \dots, p_m) = (f_1 \circ S, \dots, f_m \circ S) \cdot T$$

公開鍵は中心写像の構造を引き継ぐ

⇒ $$\left(Q_{p_1}, \dots, Q_{p_m}\right) = \left(SQ_{f_1}S^t, \dots, SQ_{f_m}S^t\right) \cdot T$$

§1.5 MPKCの攻撃の種類

分類の仕方はいろいろあるが、今回は以下のように分ける

- **Direct attack**・・・公開鍵 P とメッセージ d から署名 s を偽造する攻撃

  MQ問題 $P(x) = d$ の解 s を秘密鍵なしで直接求める

- **MinRank attack**・・・F の対称行列のランクに注目する攻撃

  $\left(Q_{p_1}, \ldots, Q_{p_m}\right) = \left(SQ_{f_1}S^t, \ldots, SQ_{f_m}S^t\right) \cdot T$ を利用してF, S, Tを復元

- **その他の攻撃**・・・秘密鍵 F の特別な構造を利用する攻撃

□ Direct attackに限らず何らかのMQ問題を解くことが多い

次が重要

(i) XLアルゴリズム[C00]

(ii) グレブナー基底アルゴリズム(F4[Fau99]など)

[C00] Courtois N. et al.: “Efficient algorithms for solving overdefined systems of multivariate polynomial equations”, Eurocrypt2000
[Fau99] Faugère, J.-C. "A new efficient algorithm for computing Gröbner bases (F4)" Journal of Pure and Applied Algebra. 139

§1のまとめ

MPKCの構成の復習

- 二次中心写像Fを線型写像S, Tで隠す　$P := T \circ F \circ S$
- MQ問題とEIP問題が安全性を支えている

二次多項式に付随する対称行列

- 変数変換と相性が良い　$\left(Q_{p_1}, \ldots, Q_{p_m}\right) = \left(SQ_{f_1}S^t, \ldots, SQ_{f_m}S^t\right) \cdot T$

MPKCの攻撃の種類

- Direct attack・・・$P(x) = d$ を解く
- MinRank attack・・・Q_{f_i}のランクに注目する
- その他の攻撃

目次

§2.1 MQ問題の解法

MPKCの多くの攻撃でMQ問題を解く必要がある:

$$g_1(x) = 0, \ldots, g_m(x) = 0$$

これはどんな方法で解けるか？その計算量は？

$$I := < g_1, \ldots, g_m >$$

主な方法

(1) XLアルゴリズム: 十分大きい D に対する $I_{\leq D}$ を線型簡約する

(2) グレブナー基底アルゴリズム: I のグレブナー基底を求める

Extended Linearization (XL)

二次方程式系 $g_1, \ldots, g_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ の解を求めたい．

$D \in \mathbb{N}$ 固定

$$G_{\leq D} := \{\, x_1^{e_1} \cdots x_n^{e_n}\, g_i \mid e_1 + \cdots + e_n \leq D-2, 1 \leq i \leq m \}$$

$G_{\leq D}$の元を適当に縦に並べる

$$g_1 = x_1^2 + 2x_1x_2 - x_2^2 + x_1 + x_2 - 1$$
$$g_2 = 2x_1^2 + x_2^2 + 2x_2 - 2$$

$$\begin{pmatrix} g_1 \\ g_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -1 & 1 & 1 & -1 \\ 2 & 0 & 1 & 0 & 2 & -2 \end{pmatrix} \begin{pmatrix} x_1^2 \\ x_1x_2 \\ x_2^2 \\ x_1 \\ x_2 \\ 1 \end{pmatrix}$$

$$G_{\leq D} = M_{\leq D} \cdot \begin{pmatrix} x_1^D \\ x_1^{D-1}x_2 \\ \vdots \\ x_n \\ 1 \end{pmatrix}$$

次数DのMacaulay行列

§2.2 XLアルゴリズム

$$G_{\leq D} = M_{\leq D} \cdot \begin{pmatrix} x_1^D \\ x_1^{D-1} x_2 \\ \vdots \\ x_n \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

⇨ **線型求解**

線型方程式 $M_{\leq D} \cdot u = 0$ を求める.
(ただし定数項に対応する u の成分は1.)

⇨ $g_1 = \cdots = g_m = 0$ の解を得る

◘正しい解を効率的に求めるには

- ➢ $M_{\leq D} \cdot u = 0$ の解空間の次元は低くなっていてほしい
  - (i) $g_1 = \cdots = g_m = 0$ の解の個数が少ないことが必要
  - (ii) 十分大きい D を選ぶ必要がある
- ➢ $M_{\leq D}$ の線型簡約の計算量を小さくしたい
  - (iii) 出来れば D を小さく取りたい

§2.3 XLの計算量評価

- $g_1 = \cdots = g_m = 0$が解を一つだけ持つとする仮定
- さらに適切な D がわかったと仮定　どうすればわかる？

⇒ 線型方程式 $M_{\leq D} \cdot u = 0$ の解空間は小さい

⇒ 計算量は $M_{\leq D} \cdot u = 0$ を解く計算量が支配的

■ XLアルゴリズムの計算量

$$3 \cdot \binom{n+D}{D}^2 \cdot \binom{n}{2}$$

線型方程式求解にはWiedemann's algorithm[W]を使う

■ Hybrid XLアルゴリズム(k個の変数に事前代入)の計算量

$$\min_{0 \leq k \leq n} 3 \cdot q^k \cdot \binom{n-k+D_k}{D_k}^2 \cdot \binom{n-k}{2}$$

[W] Wiedemann, D.: "Solving sparse linear equations over finite fields", IEEE Trans. Inform. Theory, 32(1), pp. 54–62, 1986

§2.4 Dの見積もり

Degree of regularity D_{reg} [Bardet04]

$$D_{reg} = \min\{\, d \in \mathbb{N} \mid < g_1^{top}, \ldots, g_m^{top} >_d = \mathbb{F}_q[x_1, \ldots, x_n]_d \}$$

- Semi-regularならHilbert級数 $\frac{(1-t^2)^m}{(1-t)^n}$ の正でない係数の最初の次数
  (semi-regular ≒ 特殊な構造が入っていない)
- Semi-regular でないならD_{reg}は正確に求めることは容易ではない
- その場合 D をn, mに対するsemi-regのD_{reg}で見積もることがある
- または$< g_1^{top}, \ldots, g_m^{top} >_d$のHilbert級数が計算できる場合がある

[Bardet04] M. Bardet et al., On the complexity of gr ¨obner basis computation of semi-regular overdetermined algebraic equations, ICPSS2004

§2.5 グレブナー基底アルゴリズム

- Input: $g_1, \dots, g_m \in \mathbb{F}_q[x_1, \dots, x_n]$ 二次多項式
- Output: $I \coloneqq < g_1, \dots, g_m >$ のグレブナー基底 G

1. $\mathcal{G} = \{g_1, \dots, g_m\}$, $\mathcal{S} \coloneqq \{\, S(g_i, g_j) \mid 1 \le i, j \le m \,\}$
2. $\mathcal{T}$ を $\mathcal{S}$ の中の最低次数 D の S-poly全体，$\mathcal{S} = \mathcal{S} \setminus \mathcal{T}$
3. $\mathcal{U}$: $\mathcal{T}$ を $\mathcal{G}$ でreductionしたもの
4. $\mathcal{U} = 0$ かつ $\mathcal{S} = \emptyset$ なら終了する.
5. $\mathcal{G} = \mathcal{G} \cup \mathcal{U}$ から再度 $\mathcal{S}$ を計算し、St

実験値

全ループの中で時間が掛かった次数 $D = D_{sol}$ をSolving degree[DS13]という.

このアルゴリズムの計算量はおおよそ $\binom{n + D_{sol}}{D_{sol}}^3$ と考えられる.

[DS13] Ding et al., Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields, Number Theory and Cryptography.

§2.6 D_{sol}の見積もり

First fall degree D_{ff} [DG10]

$$B := \mathbb{F}_q[x_1, \dots, x_n]/< x_1^q, \dots, x_n^q >, \quad B = \bigoplus_{d \geq 0} B_d$$

$$\varphi_d : B_{d-2}^m \ni (a_1, \dots, a_m) \longmapsto a_1 g_1^{top} + \cdots + a_m g_m^{top} \in B_d$$

$D_{ff} \in \mathbb{N}$ を $\mathrm{Ker}\,\varphi_d$ が non-trivial syzygy を含む最小値 d で定める

$(0, \cdots, -g_j, \cdots, g_i, \cdots, 0)$ と $(0, \cdots, g_i^{q-1}, \cdots, 0)$ の元で生成されない

- D_{ff} 自体の正確な値は実験で実際に確かめるくらいしかない
- その実験時間もグレブナー基底と同等くらいの時間がかかる
- non-trivial syzygyを具体的に構成してD_{ff}の上限を求める(HFE等)

[DG10] V. Dubois and N. Gama. The degree of regularity of HFE systems, ASIACRYPT2010.

§2.7 Direct attack

■ Direct attack

公開鍵とメッセージからなる
MQ問題

$p_1(x) = d_1, \ldots, p_m(x) = d_m$ の解を上記のアルゴリズムで求める攻撃

■ 計算量評価

- $\displaystyle \min_{0 \le k \le n} 3 \cdot q^k \cdot \binom{n-k+D_k}{D_k}^2 \cdot \binom{n-k}{2}$

  D_k は$(n-k)$変数m個のsemi-regular systemの D_{reg} で見積もる
  もしくは$< p_1^{top}, \ldots, p_m^{top} >_d$の次元を評価することで見積もる

- $\displaystyle \binom{n + D_{sol}}{D_{sol}}^3$

  non-trivial syzygyを具体的に構成することでD_{sol}の上限を求める

§2のまとめ

- MPKCの攻撃のいくつかは最終的にMQ問題にたどり着く
- MQ問題を解く二つの手法
  - XLアルゴリズム
  - グレブナー基底アルゴリズム
- XLアルゴリズムの計算量
  - $3 \cdot \binom{n+D}{D}^2 \cdot \binom{n}{2}$ (Dの見積もりにdegree of regularityが使われる)
- グレブナー基底の計算量
  - $\binom{n+D_{sol}}{D_{sol}}^3$ (D_{sol}の見積もりにfirst fall degreeが使われる)
- Direct attackは $P(x) = d$ を上の手法で解く攻撃

目次

§3.1 MinRank問題

■ MinRank問題

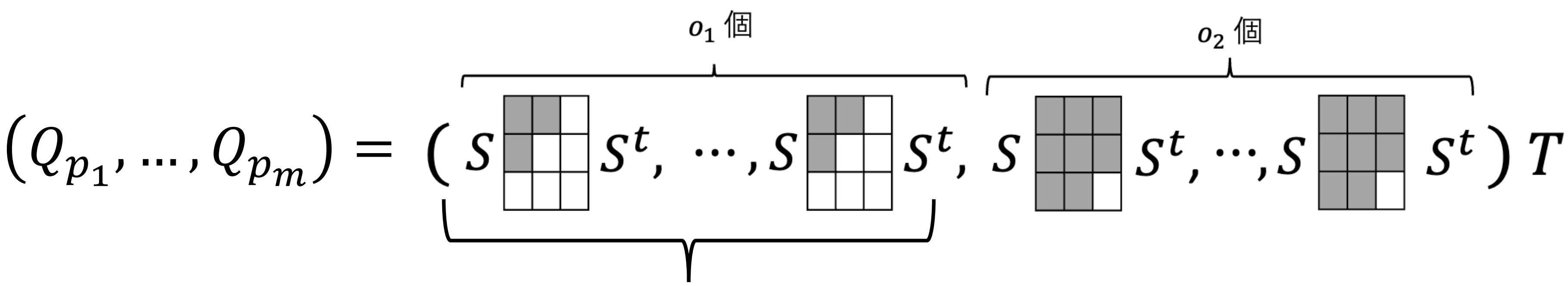
$r \in \mathbb{Z}_{>0}$, $Q_1, \ldots, Q_k \in M_{n\times n}(\mathbb{F}_q)$ k個の $n\times n$ 行列

Find $z \in \mathbb{F}_q^k$ s.t. $Q = z_1 Q_1 + \cdots + z_k Q_k$ is of rank $\leq r$

この問題はNP-hardであることが示されている

[N. Courtois, Efficient zero-knowledge authentication based on a linear algebra problem MinRank, Asiacrypt2001]

■ MinRank問題とRainbow



ここにある行列のランクは高々 $v + o_1$

$(Q_{p_1}, \ldots, Q_{p_m})$に関するMinRank問題を解くことで秘密鍵$(S, T)$が復元できる!

EIP問題の多くはMinRank問題を経由して解けるので重要!

§3.2 MinRank求解の種類

主なMinRank求解方法

(i) Brute force method

(ii) Linear search method

(iii) Kipnis-Shamir method

(iv) Minor modeling method

(v) Support minor modeling method

§3.3 Brute force method

■ MinRank問題

$r \in \mathbb{Z}_{>0}$, $Q_1, \ldots, Q_k \in M_{n\times n}(\mathbb{F}_q)$ k個の $n\times n$ 行列

Find $z \in \mathbb{F}_q^k$ s.t. $Q = z_1Q_1 + \cdots + z_kQ_k$ is of rank $\leq r$

➢ 事前にランクが r 以下になる z の個数がわかったとする

$$N := \#\{z \in \mathbb{F}_q^k \mid Rank(z_1Q_1 + \cdots + z_kQ_k) \leq r\}$$

⬇

➢ $z \in \mathbb{F}_q^k$ に対し $Rank(z_1Q_1 + \cdots + z_kQ_k) \leq r$ となる確率はN/q^k

Rankを計算する計算量は$O(n^3)$

Brute force method：ランダムなzに対するランクを何度も計算

計算量： $O\left(n^3q^k/N\right)$

§3.4 Linear search method

■ MinRank問題

$r \in \mathbb{Z}_{>0}$, $Q_1, \dots, Q_k \in M_{n\times n}(\mathbb{F}_q)$ k個の $n\times n$ 行列

Find $z \in \mathbb{F}_q^k$ s.t. $Q = z_1Q_1 + \cdots + z_kQ_k$ is of rank $\leq r$

➢ もしランダムに選んだ $v \in \mathbb{F}_q^n$ が行列 Q のkernelの元

確率 $O(1/q^r)$

⇒ $Qv = z_1 \cdot Q_1v + \cdots + z_k \cdot Q_kv = 0$

⇒ $z = (z_1, \dots, z_k)$に関する n 本の線型方程式を得る

⇒ $z \in \mathbb{F}_q^k$が求まる

Linear search method: $v \in \mathbb{F}_q^n$をランダムに選び $Qv = 0$ を解く

計算量： $O(n^3q^r)$

§3.5 Kipnis-Shamir method[K99]

$Q_1, \dots, Q_k \in M_{n\times n}(\mathbb{F}_q)$ k個の $n\times n$ 行列

$Q(z) \coloneqq z_1 Q_1 + \cdots + z_k Q_k$ としてランクが r 以下となるものを見つけたい

⇓

$Q(z)$ の右Kernelは最低でも$n-r$次元

立式

赤色の列ベクトルをKernelの基底とする

$$\underbrace{\begin{pmatrix} B_1(z,y) \\ \vdots \\ B_n(z,y) \end{pmatrix} \coloneqq Q(z) \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ y_{1,1} \\ \vdots \\ y_{r,1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{n\text{個の式}}, \underbrace{\begin{pmatrix} B_{2,1}(z,y) \\ \vdots \\ B_{2,n}(z,y) \end{pmatrix} \coloneqq Q(z) \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ y_{1,2} \\ \vdots \\ y_{r,2} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{n\text{個の式}}, \dots, \underbrace{\begin{pmatrix} B_{m-r,1}(z,y) \\ \vdots \\ B_{m-r,n}(z,y) \end{pmatrix} \coloneqq Q(z) \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ y_{1,m-r} \\ \vdots \\ y_{r,m-r} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{n\text{個の式}}$$

2次の$k+r(n-r)$変数の$n(n-r)$式数
かつ二次の部分はz変数とy変数に関してbilinear

これらはXLアルゴリズムやグレブナー基底で解かれる

[K99] Kipnis et al., Cryptanalysis of the hfe public key cryptosystem by relinearization. CRYPTO 99

§3.6 Minor modeling[F10]

$Q_1, \ldots, Q_k \in M_{n\times n}(\mathbb{F}_q)$　k個の $n\times n$ 行列

$Q(z) \coloneqq z_1 Q_1 + \cdots + z_k Q_k$ としてランクが r 以下となるものを見つけたい

⬇

$(r+1)\times(r+1)$ 小行列式が全てゼロになる z を見つければいい

- $Q_{\mathbb{a},\mathbb{b}}(z) \coloneqq$ "$Q(z)$ の $\mathbb{a},\mathbb{b}$ 部分の$(r+1)\times(r+1)$小行列",
  ただし $\mathbb{a},\mathbb{b} \subset \{1,\ldots,n\}$
- $\left\{\det Q_{\mathbb{a},\mathbb{b}}(z) = 0 \,\middle|\, \mathbb{a} \subset \{1,\ldots n\},\ \mathbb{b} \subset \{1,\ldots,n\}\right\}$
  の解はMinRank問題の解になる

$(r+1)$次のk変数の$\binom{n}{r+1}\binom{n}{r+1}$式数

高次かつ式数は多い

XLアルゴリズムやグレブナー基底で解かれる

[F10] Faugère et al., Computing loci of rank defects of linear matrices using grobner bases and applications to cryptology, ISSAC 2010

§3.7 Support minor modeling[B]

$Q_1, \dots, Q_k \in M_{n\times n}(\mathbb{F}_q)$　k個の $n\times n$ 行列

$Q(z) \coloneqq z_1 Q_1 + \cdots + z_k Q_k$ としてランクが r 以下となるものを見つけたい

⬇

それには $(r+1)\times(r+1)$ 小行列式は全てゼロになるものを見つければいい

$Q(z) = \begin{pmatrix} L_1(z) \\ \vdots \\ L_n(z) \end{pmatrix}$ と表す．$C = \begin{pmatrix} L_1(z) \\ \vdots \\ L_r(z) \end{pmatrix}$: $Q(z)$ の $r\times n$ 部分行列

(Cの中の小行列式と$L_i(z)$の成分の積の和)

➡ 各 $1 \le i \le n$, $(r+1)\times n$ 行列 $\begin{pmatrix} C \\ L_i(z) \end{pmatrix}$ の $(r+1)\times(r+1)$ 小行列式は0

➡ そこで C の中の $r\times r$ 小行列式を $c_1, c_2, \dots, c_{\binom{n}{r}}$ と適当な順番で変数化

➡ $\begin{pmatrix} C \\ L_i(z) \end{pmatrix}$ の $(r+1)\times(r+1)$ 小行列式は z_i, c_j のbilinear 多項式になる

2次の$k + \binom{n}{r}$変数の $n\binom{n}{r+1}$ 式数の bilinear equations

方程式系はXLアルゴリズムで解かれる

変数は増えたが,式数は削減される．
Bardetらは XLで解けるDの値も予測

[B] M. Bardet et al., ”Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems”, arXiv:2002.08322

§3のまとめ

- EIP問題はMinRank問題を経由して解ける場合がある

- MinRank問題を解く手法
  - (i) Brute force, (ii) Linear search, (iii) Kipnis-Shamir, (iv) Minor modeling, (v) Support minor modeling

- (iii),(iv),(v)は方程式系を解く必要がある

目次

§4.1 UOV[K99]の復習

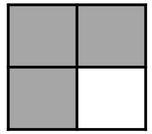
$v, o \in \mathbb{N}, n := v + o$ ただし $v > o$

次のような n 変数 o 個の二次多項式を用意する:

vinegar 変数

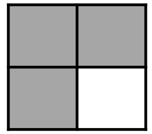
oil 変数

$$f_1(x_1, \ldots, x_n) = (x_1 \cdots x_v \ \ x_{v+1} \cdots x_n) \begin{pmatrix} a_{11}^{(1)} & \cdots & a_{1v}^{(1)} & a_{1,v+1}^{(1)} & \cdots & a_{1n}^{(1)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{v1}^{(1)} & \cdots & a_{vv}^{(1)} & a_{v,v+1}^{(1)} & \cdots & a_{vn}^{(1)} \\ a_{v+1,1}^{(1)} & \cdots & a_{v+1,v}^{(1)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{(1)} & \cdots & a_{nv}^{(1)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix}$$

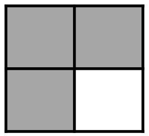
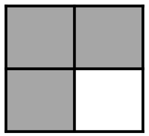
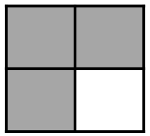


$$\vdots$$

$$f_o(x_1, \ldots, x_n) = (x_1 \cdots x_v \ \ x_{v+1} \cdots x_n) \begin{pmatrix} a_{11}^{(o)} & \cdots & a_{1v}^{(o)} & a_{1,v+1}^{(o)} & \cdots & a_{1n}^{(o)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{v1}^{(o)} & \cdots & a_{vv}^{(o)} & a_{v,v+1}^{(o)} & \cdots & a_{vn}^{(o)} \\ a_{v+1,1}^{(o)} & \cdots & a_{v+1,v}^{(o)} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}^{(o)} & \cdots & a_{nv}^{(o)} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix}$$



秘密鍵 $S \in \mathbb{F}_q^{n \times n}$, 公開鍵 $P = F \circ S = (p_1, \ldots, p_o)$ の対称行列:

$(Q_{p_1}, \ldots, Q_{p_o}) = ($ S  S^t, S  S^t, $\cdots$, S  S^t $)$

[K99] Kipnis, A., Patarin, L., Goubin, L.: “Unbalanced Oil and Vinegar Schemes”, EUROCRYPT 1999

§4.2 攻撃の種類

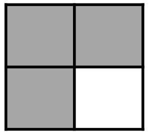
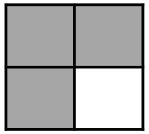
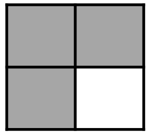
(i) UOV attack (KS attackとも)

(ii) Direct attack

(iii) Intersection attack (今回省略)

注意：UOVの中心写像の対称行列は正則行列なのでMinRank問題は起きない!

§4.3 UOV attack[K98]

$(Q_{p_1}, \dots, Q_{p_o}) = ($ S  S^t, S  S^t, $\cdots$, S  S^t $)$

$$\mathcal{O} := \left\{(0, \dots, 0, *, \dots, *) \in \mathbb{F}_q^n\right\} \cdot S^{-1}$$ Oil space

$$\mathcal{V} := \left\{(*, \dots, *, 0, \dots, 0) \in \mathbb{F}_q^n\right\} \cdot S^t$$ Vinegar space

□補題

(i) $\forall x, y \in \mathcal{O}, \quad x \cdot Q_{p_i} \cdot y^t = 0 \quad (i = 1, \dots, o).$

(ii) $\forall x \in \mathcal{O}, \quad p_i(x) = 0 \quad (i = 1, \dots, o).$

(iii) $\forall x \in \mathcal{O}, \quad x \cdot Q_{p_i} \in \mathcal{V} \quad (i = 1, \dots, o).$ (Q_{p_i}は$\mathcal{O}$を$\mathcal{V}$に写す)

(iv) $\mathcal{O}$の元が一つでも分かれば $\mathcal{O}$ は復元可能

(iv)は(i)と(ii)から言える, UOV attackは(iii)が出発点

[K98]Kipnis et al., Cryptanalysis of the Oil and Vinegar signature scheme, Crypto98

§4.3 UOV attack

$$
\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "Q_{p_i}"] & \mathbb{F}_q^n & \mathbb{F}_q^n \arrow[l, "Q_{p_j}"'] \\
\cup & \cup & \cup \\
{} \arrow[r, "\text{(iii)}"] & \mathcal{V} & \mathcal{O} \arrow[l, "\text{(iii)}"'] \\
\cup & & \cup \\
\text{If} \ \exists \mathcal{O}' \arrow[rr, leftrightarrow] & & \mathcal{O}'
\end{tikzcd}
$$

確率は $O(q^{o-v})$

➡ $Q_{p_i} \cdot Q_{p_j}^{-1}$ は $\mathcal{O}'$ を不変部分空間とする

➡ $Q_{p_i} \cdot Q_{p_j}^{-1}$ の不変部分空間を求めると $\mathcal{O}$ の元が見つかる

固有多項式の既約分解でわかる

UOV attack：公開鍵の対称行列Q_1, Q_2 をとり不変部分空間を探す

UOV attackの計算量：$\tilde{O}(q^{v-o})$ ($v = o$ では $\mathcal{O}' = \mathcal{O}$ なので多項式時間攻撃)

□Direct attack

$p_1(x)=d_1,\dots,p_o(x)=d_o$をグレブナー基底またはXLで解き, 署名を偽造する

□Direct attack計算量

- 方程式系は$n=v+o$変数、o個の二次多項式からなる
- v個の変数を適当に固定しても解は一つ存在すると考える
- 固定すると方程式系はsemi-regularにかなり近い振る舞い

$$\min_{0\le k\le o} 3\cdot q^k \cdot \binom{o-k+D_k}{D_k}^2 \cdot \binom{o-k}{2}$$

ただし, D_k は $\frac{(1-t^2)^o}{(1-t)^{o-k}}$ の正でない係数の最初の次数

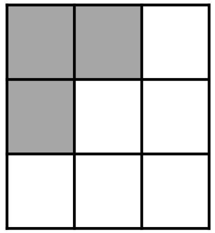
目次

■ パラメータ: $v, o_1, o_2 \in \mathbb{N}, \quad n = v + o_1 + o_2, \qquad m = o_1 + o_2$

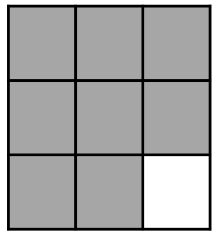
$$x = \underbrace{(x_1, \dots, x_v)}_{\text{vinegar変数}}, \quad x' = \underbrace{(x_{v+1}, \dots, x_{v+o_1})}_{\text{第一oil変数}}, \quad x'' = \underbrace{(x_{v+o_1+1}, \dots, x_n)}_{\text{第二oil変数}} \quad n\text{-変数}$$

■ <u>第一 Rainbow 多項式</u>　係数は全てランダムに選択する

$$f_1(x, x') = \sum a_{i,j}^{(1)} x_i x_{v+j} + quad\ poly.\ in\ x$$
$$\vdots$$
$$f_{o_1}(x, x') = \sum a_{i,j}^{(o_1)} x_i x_{v+j} + quad\ poly.\ in\ x$$



■ <u>第二 Rainbow 多項式</u>



$$f'_1(x, x', x'') = \sum a'^{(1)}_{i,j} x_i x_{v+o_1+j} + \sum b'^{(1)}_{i,j} x_{v+i} x_{v+o_1+j} + quad\ poly.\ in\ x, x'$$
$$\vdots$$
$$f'_{o_2}(x, x', x'') = \sum a'^{(o_2)}_{i,j} x_i x_{v+o_1+j} + \sum b'^{(o_2)}_{i,j} x_{v+i} x_{v+o_1+j} + quad\ poly.\ in\ x, x'$$

■ <u>Rainbow 中心写像</u>

$$F := (f_1, , \dots, f_{o_1}, f'_1, \dots, f'_{o_2}) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$$

[D05] Ding, J., Schmidt, D.S.: "Rainbow, a new multivariate polynomial signature scheme", ACNS 2005

§5.2 攻撃の種類

(i) UOV attack (UOVと同じ)

(ii) Direct attack (UOVと同じ)

(iii) MinRank attacks

(iv) Simple attack

Rainbow特有の構造(多層化)を
利用した攻撃(UOVには使えない)

§5.3 MinRank attacks

■ MinRank問題

$r \in \mathbb{Z}_{>0}$, $Q_1, \dots, Q_k \in M_{n\times n}(\mathbb{F}_q)$ k個の $n\times n$ 行列

Find $z \in \mathbb{F}_q^k$ s.t. $Q = z_1Q_1 + \cdots + z_kQ_k$ is of rank $\leq r$

この問題はNP-hardであることが示されている

■ MinRank問題とRainbow

$$(Q_{p_1}, \dots, Q_{p_m}) = (\underbrace{\overbrace{S\ \ S^t,\ \cdots, S\ \ S^t}^{o_1\text{個}}}, \overbrace{S\ \ S^t, \cdots, S\ \ S^t}^{o_2\text{個}})\,T$$

ここにある行列のランクは高々 $r = v + o_1$

$(Q_{p_1}, \dots, Q_{p_m})$に関するMinRank問題を解くことで秘密鍵$(S,T)$が復元できる!

§5.3 MinRank attacks

(i) Brute force method $O(n^3 q^{o_2})$

(ii) Linear search method $O(n^3 q^{v+o_1})$

(iii) Kipnis-Shamir method RBS攻撃へ(§5.4)

(iv) Minor modeling method

(v) Support minor modeling method

Rectangular MinRank attackへ(§5.5)

§5.4 RBS attack

RBS攻撃[D08]： KS方程式$\{B_{i,j}(y,z)=0\}_{\substack{1\le i\le m-r\\ 1\le j\le n}}$と$P(y)=0$の共通解を求める

[D08] Ding et al., New differential-algebraic attacks and reparametrization of rainbow, Applied Cryptography and Network Security, 2008

[P20] Ray Perlner and Daniel Smith-Tone, “Rainbow Band Separation is Better than we Thought “, IACR ePrint 2020/702

[P20]ではbi-degree XL アルゴリズムで解ける D の値を見積もった

(D,1)-degree XL　$D\in\mathbb{N}$

$$G := \{z_i p_l(y) \mid 1\le l\le m, 1\le i\le m\} \cup \{y_i B_{1,j}(y,z) \mid 1\le i\le v+o_1, 1\le j\le n\}$$

$$G_{\le D} := \{\, y_1^{d_1}\cdots y_{v+o_1}^{d_{v+o_1}}\, g(y,z) \mid g(y,z)\in G, d_1+\cdots+d_{v+o_1}\le D\}$$

線型方程式 $M_{\le D}\cdot u=0$ を求める.

[P20]では G にある種の仮定をつけることで $G_{\le D}$ のMacaulay行列 $M_{\le D}$ のランクが以下の2変数冪級数の $\boldsymbol{y}^{D+1}\boldsymbol{z}^1$ の係数に一致することを示した.

$$\frac{1-(1-\boldsymbol{y}^2)^m(1-\boldsymbol{zy})^{n-1}}{(1-\boldsymbol{y})^{v+o_1}(1-\boldsymbol{z})^m}$$

これによりRBS攻撃のより精密な計算量評価を与えた

§5.5 Rectangular MinRank attack

[B20] W. Beullens, "Improved cryptanalysis of UOV and Rainbow",
IACR ePrint 2020/1343

Rectangular MinRank Attack を提案

アイデアのコア: Beullens変形し別のMinRank問題を解く

Beullens変形　$(Q_1\ Q_2\ Q_3)$ 同じサイズの行列の組

$$Q_1 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \qquad Q_2 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \qquad Q_3 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}$$

$\Downarrow$ 変形

$$R_1 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \qquad R_2 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \qquad R_3 = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}$$

各行列の先頭列　　各行列の第2列　　各行列の第3列

$(R_1\ R_2\ R_3)$ を $(Q_1\ Q_2\ Q_3)$ の Beullens変形と呼ぶことにする

(この講演だけの名前であり、一般的な名称ではないことに注意)

§5.5 Rectangular MinRank attack

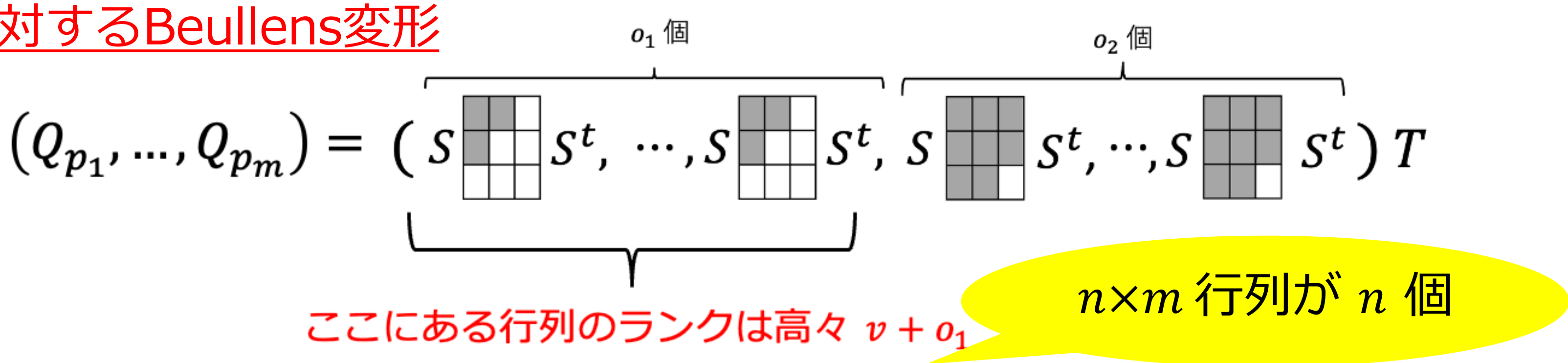
$Q_1, \ldots, Q_m \in M_{n\times n}(\mathbb{F}_q)$　　m 個の $n\times n$ 行列

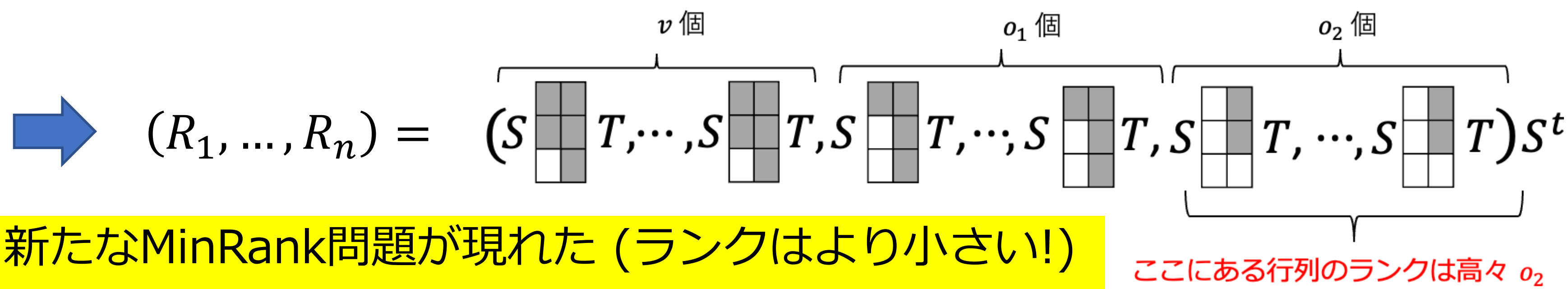
Beullens変形を $R_1, \ldots, R_n \in M_{n\times m}(\mathbb{F}_q)$ とする：

<u>簡単な補題</u>　$S \in GL_n(\mathbb{F}_q), T \in GL_m(\mathbb{F}_q)$ に対して,

$(SQ_1S^t, \ldots, SQ_mS^t) \cdot T$ のBeullens変形は $(SR_1T, \ldots, SR_nT) \cdot S^t$

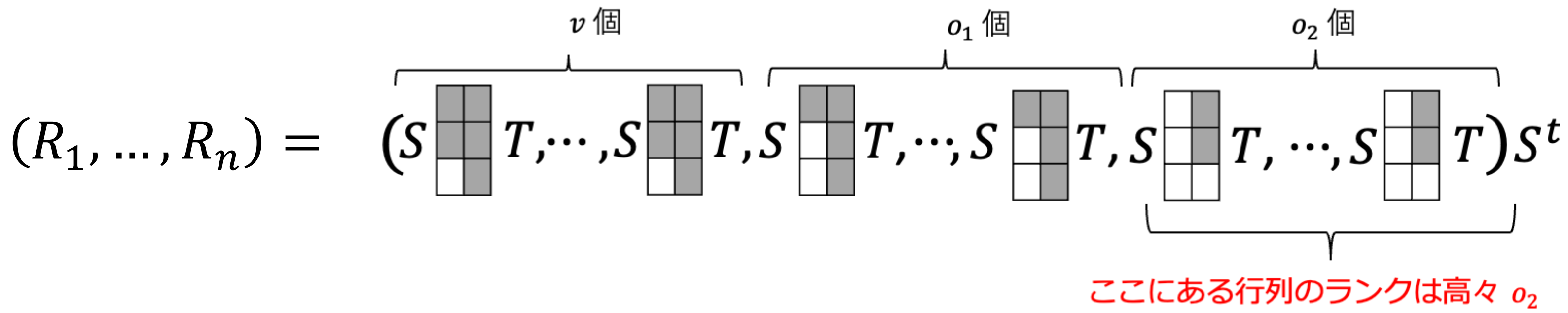
<u>Rainbowに対するBeullens変形</u>





新たなMinRank問題が現れた (ランクはより小さい!)

§5.5 Rectangular MinRank attack



このMinRank問題をSupport minor modelingで解く.

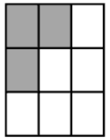
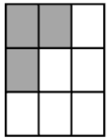
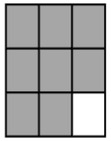
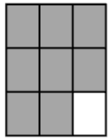
ここで, その解はDirect attack $P = 0$ の解にもなっているので

それを方程式系に加えて(bi-degree) XLアルゴリズムで計算量を求める.

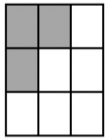
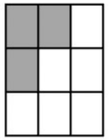
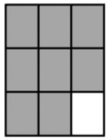
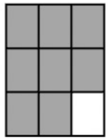
	NIST security category	parameter (q, v, o_1, o_2)	**Rectangular MinRank 攻撃**
128bit安全性	I	(16,36,32,32)	127bit安全性
196bit安全性	III	(256,68,32,48)	177bit安全性
256bit安全性	V	(256,96,36,64)	226bit安全性

§5.6 Simple attack[B22]

o_1 個　　　　　　　　o_2 個

- $(Q_{p_1}, \dots, Q_{p_m}) = ($ S  $S^t, \cdots, S$  $S^t,$ S  $S^t, \cdots, S$  $S^t)\ T$

$$\mathcal{O} := \left\{(0, \dots, 0,0, \dots, 0,*, \dots,*) \in \mathbb{F}_q^n\right\} \cdot S^{-1}$$ Oil space

- $(Q_{f_1}, \dots, Q_{f_m}) = ($  $, \cdots,$  $,$  $, \cdots ,$  $)$

$$\mathcal{O}_0 := \left\{(0, \dots, 0,0, \dots, 0,*, \dots,*) \in \mathbb{F}_q^n\right\}$$ pure Oil space

□補題

$$\Pr\left(z \leftarrow \mathbb{F}_q^n, \exists x \in \mathcal{O} \setminus \{0\}\ s.t.\ \ x \cdot Q_{p_i} \cdot z^t = 0,\ i = 1, \dots, m\right)$$
$$= \Pr\left(z \leftarrow \mathbb{F}_q^n, \exists x \in \mathcal{O}_0 \setminus \{0\}\ s.t.\ \ x \cdot Q_{f_i} \cdot z^t = 0,\ i = 1, \dots, m\right)$$
$$= \Pr\left(z \leftarrow \mathbb{F}_q^n, \exists x \in \mathcal{O}_0 \setminus \{0\}\ s.t.\ \ x \cdot Q_{f_i} \cdot z^t = 0,\ i = o_1 + 1, \dots, m\right)$$
$$\approx \Pr\left(M \leftarrow M_{o_2}(\mathbb{F}_q),\ \mathrm{Ker}(M) \neq 0\right) \approx 1/q$$ (q=16,256)

$z \in \mathbb{F}_q^n$に対し $x \cdot Q_{p_i} \cdot z^t = 0,\ (i = 1, \dots, m)$ は$1/q$の確率でOil spaceの解xを持つ

[B22]W. Beullens: Breaking Rainbow Takes a Weekend on a Laptop, Crypto'22

§5.6 Simple attack

v変数m個の二次方程式系

□Simple attack=(補題+direct attack)：

$z \in \mathbb{F}_q^n$をランダムに選び、 $x \cdot Q_{p_i} \cdot z^t = 0,\ \ p_i(x) = 0\ (i = 1, \ldots, m)$ を解く

□計算量：およそq回行えばOil spaceの元が得られるので

$$\min_{0 \le k \le v} 3 \cdot q^{1+k} \cdot \binom{v - 1 - k + D_k}{D_k}^2 \cdot \binom{v + 1 - k}{2}$$

ただし, D_k は $\frac{(1-t^2)^m}{(1-t)^{v-k}}$ の正でない係数の最初の次数

Rectangular MinRank attack	NIST security category	parameter (q, v, o_1, o_2)	Simple attack により
127bit安全性	I	(16,36,32,32)	69bit安全性
177bit安全性	III	(256,68,32,48)	157bit安全性
226bit安全性	V	(256,96,36,64)	206bit安全性

目次

§6.1 攻撃の歴史

1996年 PatarinによってHFE方式が提案される [Eurocrypt'96]

1999年 MinRank問題を使った攻撃をKipnis-Shamirが提案 [Crypto'99]

2002年 Faugèreがグレブナー基底アルゴリズムF5を方式に適用 [Crypto'03]

2004年 Bardetらがdegree of regularityを使ったF5の計算量解析 [ICPSS'04]

2010年 Dubois-Gamaがfirst fall degreeを使ってDirect attackを解析 [Asiacrypt'10]

その後、詳細な解析が進み、HFE系は非効率であることがわかった

まとめ

- MQ問題を解くアルゴリズムを解説
- MinRank問題を解くアルゴリズムを解説
- UOVの安全性解析(攻撃・評価)を解説
- Rainbowの安全性解析を解説
- HFEの歴史を簡単に説明
    - NIST PQC 標準化計画によりRainbowの解析もかなり進んだ
    - その結果、UOVが最も安全かつ効率的な方式とみなされている
    - ここ最近、UOVベースの改良方式がいくつか提案されている
    - それらの解析が今後のMPKCの課題となっている